IN THE CLAIMS:

Please amend claims 11, 12, and 13 as follows.

Claims 1-10 (canceled).

11. (currently amended) Method of encryption and decryption carried out by a plurality of encryption/decryption modules arranged in series, wherein ~~a~~ each encryption/decryption module, different from its preceding ~~the first~~ module, ~~starts~~ begins encryption/decryption operations before ~~as soon as said module receives a part of the results of encryption/decryption operations from~~ the immediately preceding encryption/decryption module has terminated its encryption/decryption operations.

12. (currently amended) Method according to Claim 11, wherein a decryption module, different from the immediately preceding ~~first~~ module, ~~starts~~ begins decryption operations as soon as said module receives a part of the results of decryption operations from the immediately preceding decryption module.

13. (currently amended) Method according to Claim 11, wherein an encryption module, different from the immediately preceding ~~first~~ module, ~~starts~~ begins encryption operations as soon as said module receives a part of the results of encryption operations from the immediately preceding encryption module.

14. (previously presented) Method according to Claim 11, carried out by three modules wherein the central module operates with a secret symmetric key.

15. (previously presented) Method according to claim 14, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys including a private key and a public key.

16. (previously presented) Method according to claim 15, wherein the first module and the last module use the private key for encryption and the public key for decryption.

17. (previously presented) Method according to claim 16, wherein the first module and the last module use the same set of private and public keys.

18. (previously presented) Method according to Claim 16, wherein the first module and the last module use a different set of private and public keys.

19. (previously presented) Method according to Claim 15, wherein, the last module uses the public key during encryption and the first module uses the private key during decryption.

20. (previously presented) Method according to Claim 11, carried out by three encryption/decryption modules, wherein all three modules operate with asymmetric keys.